What is claimed is:

1. A monitoring device disposed for thwarting denial of service attacks on a data center, the monitoring device comprising:

a device that collects statistical information on packets that are sent between a network and the data center for a plurality of customers by examining traffic as if the device was disposed on links that are downstream from links that the provisioned monitor is disposed on.

2. The monitoring device of claim 1 wherein the monitoring device is coupled to a control center through a dedicated, private network.

3. The monitoring device of claim 2 wherein the device further comprises:

a communication process that communicates statistics with the control center, and which receives queries or instructions from the control center.

4. The monitoring device of claim 1 wherein the monitoring device is a gateway device and further comprises:

a process to install filters to thwart denial of service attacks by removing network traffic that is deemed part of an attack.

5. The monitoring device of claim 1 wherein the monitoring device is a data collector device.

6. The monitoring device of claim 4 wherein the gateway comprises:

a process to aggregate traffic from the various links and to produce logs and detection heuristics.

7. A method of thwarting denial of service attacks on a victim data center coupled to a network comprises:

collecting statistical information on packets that are sent between a network and a plurality of customers of the data center by examining traffic as if the device was disposed on links that are downstream from links that the provisioned monitor is disposed on; and

communicating data, over a dedicated network, to a control center.

8. The monitoring device of claim 7 wherein the device is a gateway device, which further comprises:

installing filters to thwart denial of service attacks by removing network traffic that is deemed part of an attack.

9. The monitoring device of claim 7 wherein the monitoring device is a data collector device.

10. The monitoring device of claim 7 wherein collecting occurs for inbound and/or outbound traffic.

11. An arrangement disposed to monitor a link between a data center and a network for thwarting denial of service attacks on the data center, the arrangement comprising:

a provisioned monitor that collects statistical information for a plurality of provisioned customers, which are on links that are downstream from links that the provisioned monitor is disposed on, the provisioned monitor

maintaining separate counter logs for each provisioned customer; and

a global counter log that accounts for all traffic seen on the link that the provisioned montior is coupled to.

12. The arrangement of claim 11 wherein the gateways maintains separate packet logs for each virtual monitor.

13. The arrangement of claim 11 wherein the gateway maintains a global packet log for all traffic.

14. The arrangement of claim 11 wherein the global packet log includes a sample of all traffic seen on the link to which the gateway is connected.

15. The arrangement of claim 14 wherein packet analysis for a particular virtual monitor happens by classifying packets based on addresses at the time of the analysis.

16. The arrangement of claim 11 wherein the gateway maintains duplicate packets, keeping both a global packet log and one packet log for each virtual monitor.

17. The arrangement of claim 11 wherein gateway is a clustered gateway and includes a plurality of probes and a cluster head, with the cluster head having a process to aggregate traffic from the probes and to produce separate counter logs for each provisioned customer; and a global counter log, and produce detection heuristics.

18. The arrangement of claim 11 wherein the provisioned monitor including a virtual monitor for one for the physical

link on which the provisioned monitor is deployed is configured to be an independent node in the network capable of issuing attack warnings and responses to attack queries independently from other virtual monitors of the provisioned monitor.

19. The arrangement of claim 11 wherein the provisioned monitor including all of the provisioned monitor's virtual monitors act as one node in the distributed network.

20. The arrangement of claim 19 wherein the provisioned monitor acts as an intermediary between virtual monitors and the rest of the network and includes a process to maintain communications with the control center and to reply to attack queries.

21. The arrangement of claim 11 wherein the provisioned monitor's virtual monitors have filters installed on a per virtual monitor basis.

22. The arrangement of claim 20 wherein when a virtual monitor detects an attack on a provisioned customer, information is conveyed both to the control center and to the hosting provider's management interface.

23. The arrangement of claim 22 wherein the control center is adapted to distinguish an attack on a single provisioned customer (associated with a virtual monitor) and an attack on the link(s) on which the monitor is physically deployed.

24. A method of thwarting denial of service attacks on a victim data center coupled to a network comprises:

collecting statistical information for a plurality of provisioned customers on links that are downstream from links on which collecting occurs; and

maintaining separate counter logs for each provisioned customer; and a global counter log that accounts for all traffic seen on the links on which collecting occurs.

25. The method of claim 24 wherein collecting occurs on a gateway that passes network packets, the gateway being disposed at an edge of the network.

27. The method of claim 24 wherein collecting occurs on a data collector that samples network packets, the data collector being disposed at a location that is at a large aggregation link in the network for the data center.

28. The method of claim 24 further comprising:

performing, by the provisioned gateway, intelligent traffic analysis and filtering to identify the malicious traffic and to eliminate the malicious traffic.

29. A method of thwarting denial of service attacks on a victim data center coupled to a network comprises:

collecting statistical information for a plurality of links that are downstream from links on which collecting occurs;

performing traffic analysis on the collected statistical information on a per downstream link basis to identify malicious traffic; and

communicating alerts that arise from the traffic analysis.

30. The method of claim 28 wherein performing analysis occurs on statistical information collected for an individual one of the downstream links to identify malicious traffic intended for the individual one of the downstream links.

31. The method of claim 28 wherein communicating to a control center occurs on a downstream link basis.

32. The method of claim 28 wherein communicating occurs on a downstream link basis to a control center that determines a response to the attack.

33. The method of claim 28 wherein communicating occurs on a downstream link basis over a dedicated, hardened network to a control center that determines a response to the attack.

34. The method of claim 28 further comprising:

filtering the identified malicious traffic and to eliminate the malicious traffic from reaching the one of the downstream links.